

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-215167

(43)Date of publication of application : 04.08.2000

(51)Int.Cl.

G06F 15/00  
G06F 1/00

(21)Application number : 11-016461

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 26.01.1999

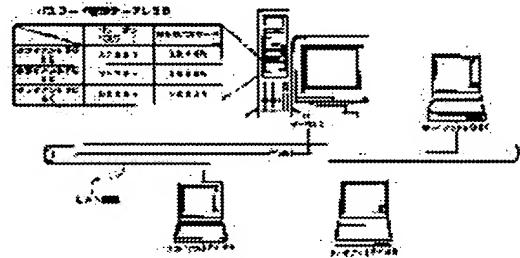
(72)Inventor : UEHARA KEIICHI  
MORISAWA SHUNICHI

## (54) COMPUTER SYSTEM AND REMOTE CONTROL METHOD OF SAME SYSTEM

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To actualize remote management while maintaining the security of a client PC by allowing a server to send a password once receiving a request when sending a wake-up indication to the client PC.

**SOLUTION:** The server 10 sends a wake-up request to client PCs 20 to 40. The client PCs 20 to 40 judge that a security function is effectively set on condition that passwords are registered, and informs the server 10 of a password request. The server 10 reads the passwords corresponding to the client PCs out of a password management table 50 and informs the clients 20 to 40 of the read-out passwords to make requests to reset the passwords. The client PCs 20 to 40 performs a setting process for an instant security mode when the passwords from the server 10 match the registered passwords.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

**BEST AVAILABLE COPY**

**THIS PAGE BLANK (USPTO)**

Copyright (C); 1998,2003 Japan Patent Office

**THIS PAGE BLANK (USPTO)**

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2000-215167  
(P2000-215167A)

(43) 公開日 平成12年8月4日(2000.8.4)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード(参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 B 5 B 0 8 5
1/00	3 7 0	1/00	3 7 0 E

審査請求 未請求 請求項の数10 O L (全 10 頁)

(21) 出願番号 特願平11-16461

(22) 出願日 平成11年1月26日(1999.1.26)

(71) 出願人 000003078

株式会社東芝  
神奈川県川崎市幸区堀川町72番地

(72) 発明者 上原 啓市

東京都青梅市末広町2丁目9番地 株式会  
社東芝青梅工場内

(72) 発明者 森沢 俊一

東京都青梅市末広町2丁目9番地 株式会  
社東芝青梅工場内

(74) 代理人 100083161

弁理士 外川 英明

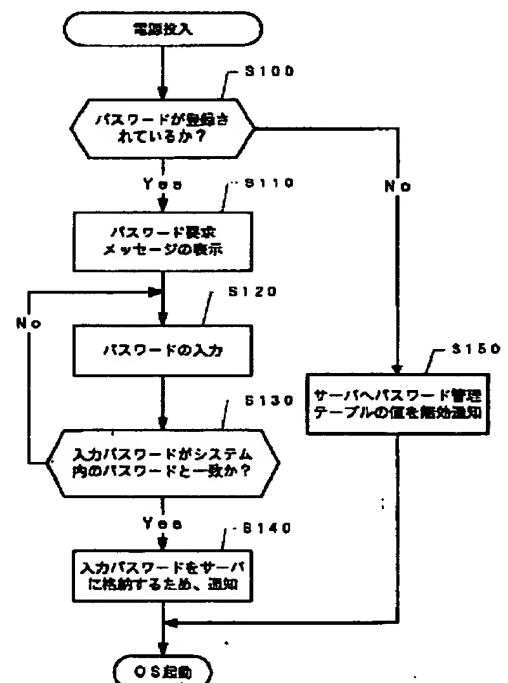
Fターム(参考) 5B085 AC02 AE03 BG07

(54) 【発明の名称】 コンピュータシステム及びそのシステムのリモート制御方法

(57) 【要約】

【課題】 十分なセキュリティを維持した状態でクライアントPCのリモート管理を実現する。

【解決手段】 PC本体やHDDの様なセキュリティ機能を持つ装置に対して、電源オン操作の制御が行われた際、キーボード等から入力されたパスワードをサーバ内のパスワード管理テーブルに格納する。サーバは、セキュリティ機能を持つ装置をWOLによりウェークアップ指示を送信する。サーバは、セキュリティ機能を持つ装置からパスワードの要求を受信すると、パスワード管理テーブルから対応するパスワードを読み出す。その後、サーバは、セキュリティ機能を持つ装置に対し、該パスワードを送信し、セキュリティ機能を持つ装置を通常の動作状態に復帰させる。



## 【特許請求の範囲】

【請求項1】 ネットワークに接続され、ネットワーク制御装置から送信されるウェークアップ信号に応答して、動作状態に復帰するウェークアップ機能を持つコンピュータ装置と、

前記コンピュータ装置は、更に、セキュリティ機能を具備し、該コンピュータ装置の電源オン操作の制御が行われた際、入力されたパスワードを前記ネットワーク制御装置に送信する手段と、

前記ネットワーク制御装置は、前記送信されたパスワードを記憶する手段を具備し、前記コンピュータ装置にウェークアップ指示を送信した時、前記コンピュータ装置からパスワードの要求を受信すると、前記記憶されたパスワードを読み出し、前記コンピュータ装置に対し、該パスワードを送信する手段とを具備することを特徴とするコンピュータシステム。

【請求項2】 前記コンピュータ装置のセキュリティ機能は、パワーオンパスワード機能、又は、アクセスロック機能であることを特徴とする請求項1記載のコンピュータシステム。

【請求項3】 前記ネットワーク制御装置の記憶する手段は、パスワード管理テーブルから構成され、前記コンピュータ装置各々から送信されたパスワードを前記パスワード管理テーブルに格納する手段とを具備することを特徴とする請求項2記載のコンピュータシステム。

【請求項4】 前記コンピュータ装置は、電源オン操作の制御が行われた際、入力されたパスワードを格納する手段とを具備することを特徴とする請求項3記載のコンピュータシステム。

【請求項5】 前記コンピュータ装置は、前記ネットワーク制御装置からパスワードを受信した時、前記コンピュータ装置内に格納されたパスワードを参照し、前記コンピュータ装置のセキュリティ機能を解除することを特徴とする請求項4記載のコンピュータシステム。

【請求項6】 ネットワークに接続され、ネットワーク制御装置から送信されるウェークアップ信号に応答して、動作状態に復帰するウェークアップ機能を持つコンピュータシステムに於いて、

前記コンピュータ装置は、セキュリティ機能を具備し、該コンピュータ装置の電源オン操作の制御が行われた際、入力されたパスワードを前記ネットワーク制御装置に送信する手段と、

前記ネットワーク制御装置から前記コンピュータ装置にウェークアップ指示が送信された時、前記ネットワーク制御装置に対し、パスワード要求を送信する手段と、パスワード要求を送信後、前記ネットワーク制御装置からパスワードを受信する手段とを具備することを特徴とするコンピュータシステム。

【請求項7】 前記コンピュータ装置のセキュリティ機能は、パワーオンパスワード機能、又は、アクセスロッ

ク機能であることを特徴とする請求項6記載のコンピュータシステム。

【請求項8】 前記コンピュータ装置は、該コンピュータ装置の電源オン操作の制御が行われた際にパスワードが登録されていない場合、前記ネットワーク制御装置にパスワード消去・無効の要求を送信する手段とを具備することを特徴とする請求項7記載のコンピュータシステム。

【請求項9】 前記コンピュータ装置は、前記ネットワーク制御装置からパスワードを受信した時、前記コンピュータ装置内に格納されたパスワードを参照し、前記コンピュータ装置のセキュリティ機能を解除することを特徴とする請求項8記載のコンピュータシステム。

【請求項10】 ネットワークに接続され、ネットワーク制御装置から送信されるウェークアップ信号に応答して、動作状態に復帰するウェークアップ機能を持つコンピュータ装置で使用するリモート制御方法に於いて、前記コンピュータ装置は、更に、セキュリティ機能を具備し、該コンピュータ装置の電源オン操作の制御が行われた際、入力されたパスワードを前記ネットワーク制御装置に送信するステップと、

前記ネットワーク制御装置は、前記送信されたパスワードをパスワード管理テーブルに記録するステップと、前記ネットワーク制御装置は、前記コンピュータ装置にウェークアップ指示を送信した時、前記コンピュータ装置からパスワードの要求を受信するステップと、前記ネットワーク制御装置は、前記パスワード管理テーブルから前記パスワードを読み出し、前記コンピュータ装置に対し、該パスワードを送信するステップとを具備することを特徴とするコンピュータシステムのリモート制御方法。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 この発明は、コンピュータシステムのリモート制御に係わり、特に、サーバからの特定のバケット受信に応答して、停止状態、又は、スリープ状態のクライアントを通常動作状態に復帰するコンピュータシステムのリモート制御に関する。

## 【0002】

【従来の技術】 近年、企業内のパーソナルコンピュータ（PC）を集中管理するために、サーバから各PCをリモート制御するためにDesktop Management Interface（DMI）と称される標準インターフェース仕様に基づき、デスクトップPCの開発が行なわれている。

【0003】 上記DMIに基づき、サーバからのリモート制御でデスクトップPCを電源オンさせる「Wake-On-LAN（WOL）」およびデスクトップPCの異常をサーバに自動的に通知する「Alert-On-LAN（AOL）」と呼ばれる機能を搭載したデスク

ップPCが製品化されている。

【0004】WOLを用いた典型的なリモート管理の形態は、企業内の情報化ツールとして従業員各々の机上にデスクトップPCを配置し、これらをLocal Area Network (LAN) を介してサーバと結んだ動作環境とする。各デスクトップPCにインストールされているソフトウェアをバージョンアップする際や、各デスクトップPCからデータを収集する場合、サーバおよび従業員各々のデスクトップPCを管理する部門は、例えば、特定の日の退社時に各デスクトップPCをWOLできる状態にして帰宅するように各従業員に求める。管理部門は、その深夜、サーバから特別なパケットを各デスクトップPCに送信し、電源オフ状態、又は、スリープ状態にある各デスクトップPCを自動的に立ち上げてソフトウェアのバージョンアップとデータ収集処理を行う。

【0005】このようにサーバからのリモート制御で企業内の各デスクトップPCを集中管理することができる。通常、PC本体には、第三者による不正使用を防止するために、パワーオンパスワード機能が設けられている。このパワーオンパスワード機能に於いては、PC本体の電源投入時にPCのユーザによって入力されたパスワードをチェックし、所定のパスワードが入力された時にのみPC本体のシステムを起動可能とする。このパスワード機能の有効／無効は、ユーザによるパワーオンパスワードの登録・登録解除操作などによって行われる。

【0006】また、PCには、第三者によるHDDの不正抜き取りによる使用を防止するために、アクセスロック機能が設けられている。このアクセスロック機能に於いて、オペレーティングシステム(OS)がPCのスリープ状態を管理する場合、自動的に、HDDに供給される電源がオフされるため、HDDに供給される電源オフにより、HDDはアクセスロック状態になる。HDDのアクセスロック状態の解除には、再度、ユーザは、HDDパスワードを入力する。このアクセスロック機能の有効／無効も、ユーザによるHDDパスワードの登録・登録解除操作などによって行われる。

【0007】上記パワーオンパスワード機能とアクセスロック機能が有効状態に設定されると、PC本体やHDDに電源が投入されても正しいパスワードが入力されない限り、PCのシステム状態は通常の動作状態に復帰されない。従って、PC本体が起動できず、HDDに格納された機密情報などが第三者に漏洩されるといった事態を防止できるので、PCのセキュリティを維持することができる。

【0008】

【発明が解決しようとする課題】しかしながら、上記した従来技術では、PCのパワーオンパスワード機能やアクセスロック機能を有効に設定してしまうと、今度は、WOLによるPCを夜間に電源オンしても、正当なパス

ワードを入力しない限り、PCのシステム状態は通常の動作状態に復帰できない。この為、サーバからのリモート制御でクライアントPCを無人でスタートさせるというWOL本来の性能が損なわれてしまう。

【0009】そこで、本発明は上記の問題を解決するためになされたものであり、クライアントPCの十分なセキュリティを維持した状態で、前述のリモート管理を実現することができるコンピュータシステム及びそのシステムのリモート制御方法を提供することを目的とする。

【0010】

【課題を解決するための手段】この発明は、ネットワークに接続され、ネットワーク制御装置から送信されるウェイクアップ信号に応答して、動作状態に復帰するウェイクアップ機能を持つコンピュータ装置と、前記コンピュータ装置は、更に、セキュリティ機能を具備し、該コンピュータ装置の電源オン操作の制御が行われた際、入力されたパスワードを前記ネットワーク制御装置に送信する手段と、前記ネットワーク制御装置は、前記送信されたパスワードを記憶する手段を具備し、前記コンピュータ装置にウェイクアップ指示を送信した時、前記コンピュータ装置からパスワードの要求を受信すると、前記記憶されたパスワードを読み出し、前記コンピュータ装置に対し、該パスワードを送信する手段とを具備したことを特徴とする。

【0011】また、本発明の前記コンピュータ装置のセキュリティ機能は、パワーオンパスワード機能、又は、アクセスロック機能であることを特徴とする。このような構成によれば、クライアントPCの各種パスワード登録時、ネットワーク制御装置にも同じパスワードを管理・格納するので、WOLの為に、クライアントPCのパスワードを解除なしに、クライアントPCの十分なセキュリティを維持した状態で、リモート管理を実現することができる。

【0012】また、本発明の前記ネットワーク制御装置の記録する手段は、パスワード管理テーブルであり、前記コンピュータ装置各々から送信されたパスワードを前記パスワード管理テーブルに格納する手段とを具備することを特徴とする。

【0013】このような構成によれば、ネットワーク制御装置は、各種クライアントPCのパスワードを一元的に管理でき、クライアントPCのパスワードが、ユーザによって、登録・更新する度に、ネットワーク制御装置のパスワード管理テーブルの対応する箇所にクライアントPCのパスワードを更新できる。

【0014】また、本発明のコンピュータ装置は、電源オン操作の制御が行われた際、入力されたパスワードを格納し、ネットワーク制御装置からパスワードを受信した時、コンピュータ装置内に格納されたパスワードを参照し、コンピュータ装置のセキュリティ機能を解除することを特徴とする。

【0015】このような構成によれば、ネットワーク制御装置のパスワード管理テーブルから読み出されたパスワードをとコンピュータ装置のパスワードと容易に照合することが可能となる。

【0016】更に、この発明は、ネットワークに接続され、ネットワーク制御装置から送信されるウェークアップ信号に応答して、動作状態に復帰するウェークアップ機能を持つコンピュータ装置に於いて、前記コンピュータ装置は、セキュリティ機能を具備し、該コンピュータ装置の電源オン操作の制御が行われた際、入力されたパスワードを前記ネットワーク制御装置に送信する手段と、前記ネットワーク制御装置から前記コンピュータ装置にウェークアップ指示が送信された時、前記ネットワーク制御装置に対し、パスワード要求を送信する手段と、パスワード要求を送信後、前記ネットワーク制御装置からパスワードを受信する手段とを具備することを特徴とする。

【0017】また、本発明は、前記コンピュータ装置のセキュリティ機能は、パワーオンパスワード機能、又は、アクセスロック機能であることを特徴とする。このような構成によれば、パスワードが登録されているクライアントPCにおいて、WOLの為に、クライアントPCのパスワードを解除なしに、クライアントPCの十分なセキュリティを維持した状態で、リモート管理を実現することができる。

【0018】また、更に、本発明のコンピュータ装置は、コンピュータ装置の電源オン操作の制御が行われた際、パスワードが登録されていない場合、前記ネットワーク制御装置にパスワード消去・無効の要求を送信する手段とを具備することを特徴とする。このような構成によれば、ネットワーク制御装置のパスワード管理テーブルを参照すれば、クライアントPCのセキュリティ機能を管理することができる。

【0019】

【発明の実施の形態】以下、図面を参照してこの発明の実施形態を説明する。図1には、本発明の一実施形態に係わるネットワークに接続された各コンピュータシステムが示されている。このコンピュータシステムは、Local Area Network (LAN) 上に接続されたサーバ10と、複数のクライアントPC20～40から構成されている。サーバ10は、各クライアントPC20～40間とのネットワーク管理および、DMIを介して、ネットワークに接続された各クライアントPCのリモート制御を行う。更に、サーバPC10は、WOLを利用して、各クライアントPC20～40をリモート制御する為、各クライアントPC20～40毎(ごと)のパスワードを管理するパスワード管理テーブル50を具備している。このパスワード管理テーブル50には、各クライアントPC20～40毎のパワーオンパスワードとHDDパスワード等のパスワードデータを格納

する。サーバ10は、パスワード管理テーブル50に格納された各パスワードデータを読み出し、パワーオンパスワード機能およびアクセスロック機能を有する各クライアントPC20～40のパスワードを解除し、WOLによる各クライアントPC20～40にインストールされたソフトウェアをバージョンアップおよび各クライアントPC20～40からのデータ収集を行う。

【0020】図2には、本発明の一実施形態に係わるクライアントPCのシステム構成が示されている。このクライアントPCのシステムは、ノートブックタイプまたはサブノートタイプのポータブルパーソナルコンピュータである。ポータブルパーソナルコンピュータは、コンピュータ本体と、このコンピュータ本体に開閉自在に取り付けられたLCDパネルユニットから構成されている。

【0021】ポータブルパーソナルコンピュータ本体には、PCIバス、ISAバス、CPUモジュール60、主メモリ70、VGAコントローラ80、ビデオメモリ(VRAM)90、PCIインターフェイスブリッジ(PCI I/F)100、I/Oコントローラ110、フロッピーディスクドライブ(FDD)120、ハードディスクドライブ(HDD)130、フラッシュBIOS-ROM140、キーボードコントローラ(KBC)160、LANコントローラ170などが設けられている。

【0022】CPUモジュール60は、このシステム全体の動作制御およびデータ処理を実行するものであり、ここにはCPU、キャッシュ、さらには主メモリ70を制御するためのメモリコントローラなどが搭載されている。

【0023】主メモリ70は、このシステムの主記憶として使用されるものであり、オペレーティングシステム、処理対象のアプリケーションプログラム、およびアプリケーションプログラムによって構成されたユーザデータ等が格納されている。

【0024】VGAコントローラ80は、このシステムのディスプレイモニタとして使用されるLCDおよび外部CRTを制御するためのものであり、VRAM90に描画された画面データをそれらディスプレイモニタに表示する。

【0025】PCIインターフェイスブリッジ(PCI I/F)100は、1チップLSIによって実現されたゲートアレイであり、ここには、PCIバスとISAバスとの間を双方向で接続するブリッジ機能が内蔵されているほか、HDD130の制御を行うIDEコントローラなども内蔵されている。

【0026】I/Oコントローラ110は、各種I/Oデバイスを制御するためのゲートアレイであり、PCMCI A/CARD BUS仕様のPCカードを制御する機能および、FDD120を制御する機能の他、シリア



ルポート、パラレルポート、赤外線通信ポートなどの制御機能を有している。パワーオンパスワード登録時にFDD120にフロッピーディスク(FD)を装着しておくと、そのFDに登録パスワードが保存される。

【0027】フラッシュBIOS-ROM140は、システムBIOS(Basic I/O System)を記憶するためのものであり、プログラム書き換えが可能のようにフラッシュメモリによって構成されている。システムBIOSは、このシステム内の各種ハードウェアをアクセスするためのファンクション実行ルーチンを体系化したものであり、ここには、パワーオンパスワードおよびHDDパスワードおよびインスタントセキュリティなどの機能も含まれる。登録された各種パスワードは、フラッシュBIOS-ROM140内の所定の記憶領域であるパスワードブロック150に書き込まれる。

【0028】フラッシュBIOS-ROM140内にパワーオンパスワードが登録されている場合には、システムがパワーオンされても、そのフラッシュBIOS-ROM140内に登録されているパスワードと同じパスワードが、キーボード(KB)操作によってユーザから入力されるまで、OSの起動や、サスペンドモードからの復帰は禁止されている。

【0029】また、システムのパワーオン、ハイパーネーションまたはサスペンドモード・レジュームからの復帰時でのPCのHDDの電源供給時、システムBIOSは、HDDパスワードがHDD130内のEEPROMに登録されている、即ち、HDDがアクセスロック状態であると判定した場合、HDDパスワードと同じパスワードが、キーボード(KB)操作によってユーザから入力されるまで、HDDへの読み出し・書き込みアクセスが禁止される。

【0030】フラッシュBIOS-ROM140には、システム環境設定を変更するためのセットアッププログラムも格納されており、所定のキー操作を行うことによりそのセットアッププログラムを起動することができる。パワーオンパスワードおよびHDDパスワード(以下、パスワードと称す)の登録および解除は、フラッシュBIOS-ROM140のセットアッププログラム、あるいは外部FDなどによって供給されるセットアッププログラムを起動することによって行うことができる。

【0031】フラッシュBIOS-ROM140あるいは外部FDなどからセットアッププログラムを起動すると、システムセットアップメニュー画面が表示される。パスワードが登録されていない場合には、システムセットアップメニュー画面上のパスワードの設定項目「PASSWORD」には、「NOT Registered」と表示されている。システムセットアップメニュー画面上でパスワード設定項目「PASSWORD」にカーソルを合わせてスペースキーを押すことにより、パスワード登録を要求することがでる。入力可能なパスワード

は、例えば、英数文字で10桁までに制限されている。

【0032】パスワードが入力された場合、再度、確認のためにパスワードの入力がユーザに要求される。ユーザによって再度入力されたパスワードが先に入力されたパスワードと一致すると、その入力パスワードがフラッシュBIOS-ROM140のパスワードブロック150およびHDD130のEEPROM内に保存される。これによって、PCのシステムにパスワードが登録されたことになる。

【0033】キーボードコントローラ(KBC)160は、キーボード(KB)、およびポインティングスティック(PS)またはマウスなどのポインティングデバイスの制御を行う。

【0034】LANコントローラ170は、前述のWOL機能およびAOL機能に対応し、LAN回線を介して他のクライアントPC20~40およびサーバ10と通信する。WOL機能が、クライアントPCのセットアッププログラム上で有効に設定されている場合、LANコントローラ170はLAN回線を介してサーバ10から特定の packets を介して受信した時、クライアントPC本体20~40を自動的に電源オンするためのウェイクアップ信号を発生する。また、クライアントPC本体20~40でAOL機能が有効に設定されている場合、LANコントローラ170はLAN回線を介してクライアントPC本体20~40の異常等をサーバ10に自動通知する。

【0035】次に、図3を参照して、クライアントPCのパスワードをサーバのパスワード管理テーブルに登録する操作手順を説明する。クライアントPCがユーザ、又は、オーナーによってパワーオンされると、システムBIOSにより以下の処理が行われる。

【0036】まず、フラッシュBIOS-ROM140のパスワードブロック150内にパスワードが存在するか否かを調べることにより、システム内にパスワードが登録されている状態であるか否かが判定される(ステップS100)。パスワードブロック150内にパスワードが登録されている場合(ステップS100のYes)、システムBIOSは、クライアントPCのディスプレイ上にパワーオンパスワードやHDDパスワードの入力要求メッセージを表示する(ステップS110)。

【0037】システムBIOSはパスワードブロック150内にパスワードが登録されていないと判定した場合、サーバ10にパスワード管理テーブルに格納されたパスワードデータを消去、又は、無効する様に通知後、クライアントPCのHDDにインストールされたOSを起動する(ステップS100のNo→ステップS150)。サーバ10は、クライアントPCからパスワード管理テーブル50のパスワードデータを消去、又は、無効する通知を受信した時、各クライアントPCに対応するパスワードデータとして、例えば、「0000h」を

示すパスワード未登録データを格納する。

【0038】次に、クライアントPCのディスプレイ上にパワーオンパスワードやHDDパスワードの入力要求メッセージが表示された場合、クライアントPCのユーザは、キーボードを利用して、パワーオンパスワードを入力する（ステップS120）。システムBIOSは、入力されたパワーオンパスワードとパスワードブロック150内の登録パスワードとの照合を行う（ステップS130）。入力されたパワーオンパスワードとパスワードブロック150内の登録パスワードが一致すれば（ステップS130のYes）、システムBIOSはLAN回線を介してサーバ10に入力されたパワーオンパスワードを通知する。サーバ10は、クライアントPCから通知されたパワーオンパスワードをパスワード管理テーブル50の所定位置に格納する（ステップS140）。

【0039】上記パワーオンパスワードの入力・照合と同様に、クライアントPCの電源投入に伴うパスワード入力の時点で、クライアントPCのセットアッププログラムにより、HDD130のEEPROMに既に格納されているHDDパスワードと入力されたHDDパスワードを照合する（ステップ130）。システムBIOSは、入力されたHDDパスワードとパスワードブロック150内の登録パスワードが一致すれば、入力されたHDDパスワードをパスワードブロック150に格納し、サーバ10に入力されたHDDパスワードを通知する。サーバ10は、クライアントPCから通知されたHDDパスワードをパスワード管理テーブル50の所定位置に格納する（ステップS140）。

【0040】HDDパスワードもクライアントPCのセットアッププログラムの処理時点で、パワーオンパスワードと同様に、パスワードブロック150に格納することもできる。この場合、クライアントPCの電源投入時、HDDパスワードをパスワードブロック150に格納しないで、サーバ10に通知するだけで良い。

【0041】システムBIOSは、サーバ10にパスワードを通知後、サーバ10からパスワード登録通知を受信すると、クライアントPCのOSを起動する。また、システムBIOSは、パスワードブロック150に登録されているパスワードが入力されたパスワードと一致しないと判定した場合（ステップS130のNo）、システムBIOSは再度パスワード入力画面をディスプレイ上に表示し、ユーザにパスワード入力を促す。システムBIOSはパスワード解除のための試行回数が所定値（例えば、3回）に達したと判断した場合、エラー処理、例えば、クライアントPCの電源をオフし、以降の操作を禁止する。

【0042】図4には、サーバからクライアントPCのリモート制御処理の手順を示す。図5には、クライアントPCのウェークアップ制御処理の手順を示す。次に、図4と図5を参照して、クライアントPCがサーバから

のWOLによって電源オンされた場合、クライアントPCのセキュリティ状態を解除する手順を説明する。

【0043】企業内の各従業員机上のクライアントPC20～40にインストールされているソフトウェアをバージョンアップする際および、各クライアントPC20～40のHDDからデータを収集する場合、管理部門では特定の日の退社時に各クライアントPCをWOLができる状態にして帰宅するように従業員に求める。その深夜、サーバ10から特別なパケットを各クライアントPC20～40に通知し、ウェークアップの要求を行う（ステップS200）。

【0044】各クライアントPC20～40は、電源オンされた停止状態、又は、スリープ状態からウェークアップすると、システムBIOSは、まず、ウェークアップ要因をチェックする（ステップS300）。システムBIOSは、LANコントローラ170からのウェークアップ信号Wake\_Upによるものであるか、通常の電源スイッチ操作によるものであるか判別する（ステップS310）。

【0045】LANコントローラ170からのウェークアップ信号Wake\_Upによるウェークアップ要求であれば（ステップS410のYes）、システムBIOSはパスワードブロック150内にパワーオンパスワードやHDDパスワードなどのパスワードが登録されているか否かを調べる。登録されていれば、システムBIOSはパワーオンパスワードやHDDパスワードのようなパスワードチェック（セキュリティ）機能が有効設定されていると判断し、LAN回線を介して、サーバ10にパワーオンパスワードやHDDパスワードなどのパスワード要求を通知する（ステップS320）。

【0046】また、ウェークアップ要因がユーザによる電源スイッチ操作であったならば、システムBIOSは図3記載のステップS100以降の手順を実行する（ステップS310のNo）。

【0047】クライアントPCからパスワード要求を受信したサーバ10は、ウェークアップ信号を通知したクライアントPCにパスワードが登録されていると判断する（ステップS210）。サーバ10は、パスワード管理テーブル50からクライアントPCに対応したパワーオンパスワードやHDDパスワードなどの各種パスワードデータを読み出す（ステップ210のYes～ステップS220）。

【0048】サーバ10は、パスワードを要求した各種クライアント20～40にPCパスワード管理テーブル50から読み出されたパスワードを通知し、パスワード解除の要求を行う（ステップS230）。

【0049】クライアントPC20～40は、サーバ10からパスワード解除の要求を受信すると、サーバ10からのパスワードがクライアントPCのパスワードブロック150内の登録パスワードと一致するか否かを判定す

る(ステップS330)。登録パスワードと一致する場合(ステップS330のYes)、クライアントPCのシステムBIOSは、パスワード解除の成功をサーバ10に通知する。その後、クライアントPCのシステムBIOSは、以下のようなインスタントセキュリティモードの設定処理を行う(ステップS340)。

【0050】即ち、システムBIOSは、まず、KBC160にキーロックコマンドを転送し、キーロックを指示する。このコマンドに応答して、KBC160は、全ての入力デバイス、つまり、キーボード、外部キーボードおよびマウスをロックする。これにより、KBC160による通常のキーコード送信は、行われなない。次いで、システムBIOSは、LCDパネル内のバックライトを制御する回路にコマンドを転送し、LCDパネルなどのディスプレイモニターの表示画面をブランクさせる。この画面ブランクは、LCDパネルのバックライトを消灯することによって行うことができる。

【0051】このように表示画面をブランクし、且つ、キーロックした状態で、システムBIOSは、サーバ10にパスワード解除の成功を通知し、クライアントPCのサスペンド・ハイパーネーションからの復帰処理、あるいは、通常のOSの起動を行う。これにより、サーバ10は、クライアントPC20~40からパスワード解除の成功の通知を受信後(ステップS240のYes)、ネットワークを介してクライアントPC20~40をアクセスする。

【0052】一方、システムBIOSは、サーバ10からのパスワードが、クライアントPCのパスワードブロック150に登録されているパスワードと一致しないと判定した場合、サーバ10に対しパスワード要求を通知する(ステップS330のNo)。

【0053】システムBIOSは、サーバ10からパスワード解除要求に従い、サーバ10から送付されたパスワードをパスワード解除試行の実行を所定回数後、パスワードブロック150内の登録されたパスワードと一致しなければ、サーバ10にパスワード解除の不成立を通知する。

【0054】サーバ10は、パスワード解除の不成立を通知する受信後、エラー処理、例えば、ユーザがクライアントPCの電源スイッチ操作に伴う起動時、WOLエラーメッセージを通知する準備を行う(ステップS240のNo)。

【0055】また、サーバ10が、ウェイクアップ信号を通知したクライアントPCからパスワード要求を受信しなかったならば、クライアントPCにパスワードが登録されていないと判断し、クライアントPCのサスペンド・ハイパーネーションからの復帰処理、あるいは、OS起動後、クライアントPCのHDDにアクセスを実行する(ステップS210のNo)。

【0056】本願発明の様な構成にするからこそ、シス

テムBIOSのセットアップ処理によるパスワード登録後、クライアントPCの電源スイッチの操作に伴うユーザから入力されたパスワードの度毎に、サーバ10に入力パスワードを通知し、パスワード管理テーブル150のパスワードデータを更新することができる。従って、クライアントPCのパスワードを常に最新のものとして、サーバ10がクライアントPCのセキュリティ管理を維持しながらリモート制御できる。

【0057】尚、本願発明の実施形態では、クライアントPCのシステムをノートブックタイプ、またはサブノートタイプのポータブルパーソナルコンピュータで示したが、同様に、デスクトップタイプのパーソナルコンピュータでもクライアントPCを構成できる。

【0058】更に、本願発明の実施形態では、システムBIOSのセットアップ処理によるパスワード登録後、クライアントPCの電源スイッチの操作に伴うユーザから入力されたパスワードをサーバ10に通知し、パスワード管理テーブルに格納しているが、システムBIOSのセットアップ処理によるパスワード登録時、パスワードをサーバ10に通知し、パスワード管理テーブルに格納することもできる。

【0059】また、上記実施形態では、クライアントPC毎にネットワークパスワードが割り当てられているならば、クライアントPCの電源スイッチの操作時、ユーザが入力したネットワークパスワードをサーバ10のパスワード管理テーブルに格納することも出来る。

【0060】また、更に、上記実施形態では、サーバからクライアントPCのリモート制御で、サーバからクライアントPCにパスワードを送信する時、クライアントPCのパスワードブロックにパワーオンパスワードやHDDパスワードなどの複数のパスワードデータが登録されていても、サーバから送信されたパスワードデータのうちのいずれか一つに一致するならば、クライアントPCはインスタントセキュリティ処理を実行することもできる。

【0061】

【発明の効果】以上説明したように、この発明によれば、クライアントPCの十分なセキュリティを維持した状態で、サーバからのリモート管理を実現することができる。

【図面の簡単な説明】

【図1】本発明の一実施形態に係わるネットワークに接続された各コンピュータシステムを示す図。

【図2】同実施形態に係わるクライアントPCのシステム構成を示すブロック図。

【図3】同実施形態のクライアントPCのパスワードをサーバのパスワード管理テーブルに登録する手順を示すフローチャート。

【図4】同実施形態のサーバからクライアントPCのリモート制御処理の手順を示すフローチャート。

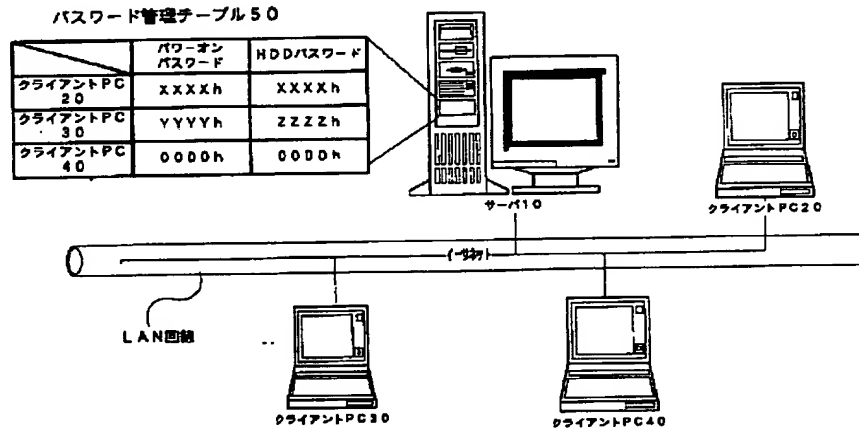
【図5】同実施形態のクライアントPCのウェークアップ制御処理の手順を示すフローチャート。

【符号の説明】

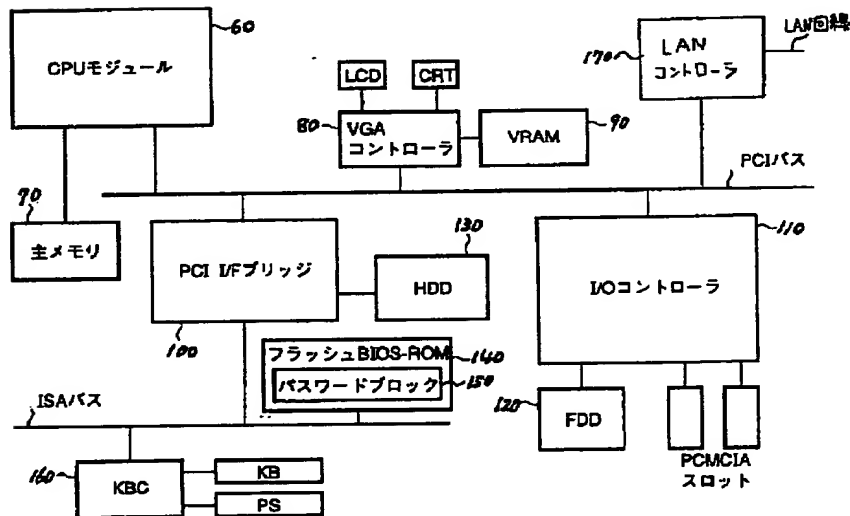
10…サーバ、20～40…クライアントPC、50…パスワード管理テーブル、60…CPU、70…主メモ

リ、80…VGAコントローラ、90…VARM、100…PCIインターフェースブリッジ装置、110…I/Oコントローラ、120…FDD、130…HDD、140…フラッシュBIOS、150…パスワードブロック、160…KBC、170…LANコントローラ

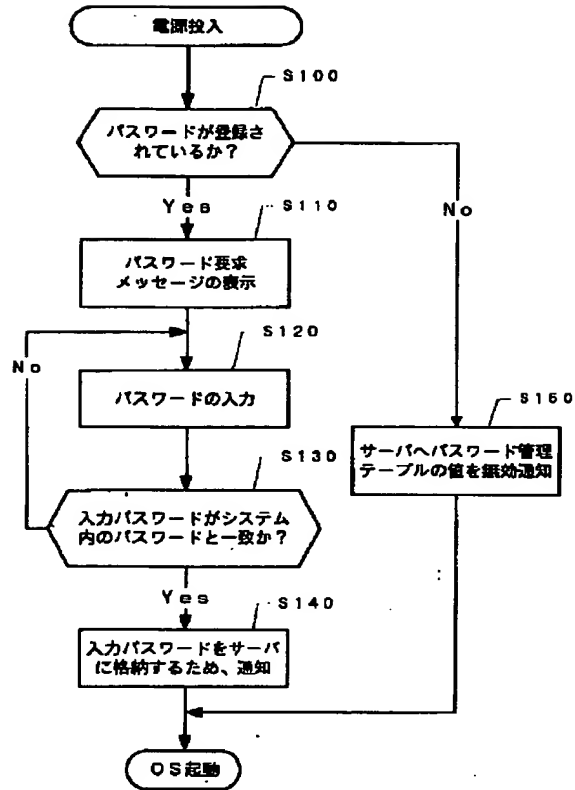
【図1】



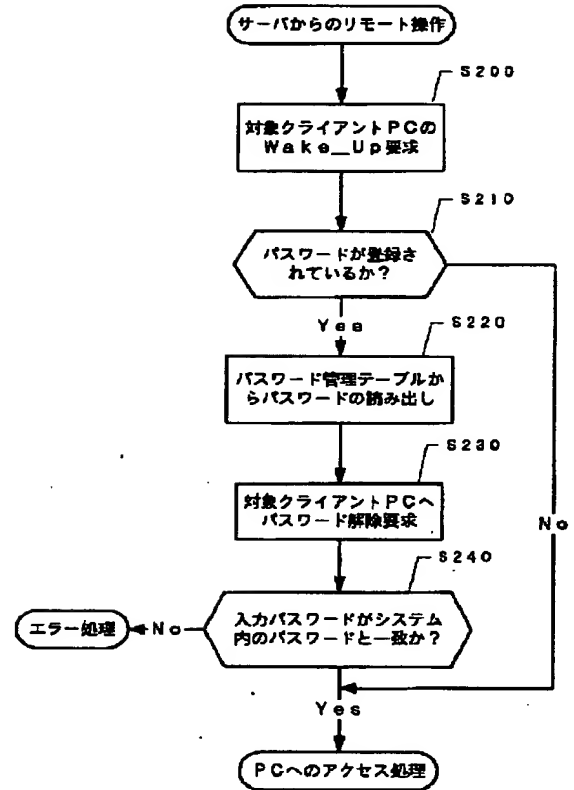
【図2】



【図3】



【図4】



【図5】

